Oblivious transfer, the CHSH game, and quantum encodings

André Chailloux* Iordanis Kerenidis† Jamie Sikora‡

April 4, 2013

Abstract

Quantum information studies how information is encoded and decoded in quantum mechanical systems. In this paper, we study the basic scenario where two classical bits are encoded into a quantum state. We prove a "learning lemma," which provides a new upper bound on the average probability of decoding each bit that depends on the probability of learning the XOR of the two bits. Moreover, we give bounds on how well each bit can be decoded when their XOR is hidden and generalize these concepts to strings.

Our learning lemmata have strong connections to cryptography and nonlocality. In particular, we show a set of equivalences between secure oblivious transfer protocols, CHSH-type games, and quantum encodings hiding the XOR. These equivalences allow us to use results in one area to prove results in another. For example, we use information bounds to give bounds on the values of CHSH-type games and also on the "correctness" of certain secure oblivious transfer protocols. We also use results of quantum XOR games to show that secure oblivious transfer admits perfect parallel repetition. Last, our learning lemmata enable us to improve the lower bounds on the cheating probabilities of any quantum oblivious transfer protocol.

1 Introduction

Quantum information studies how information is encoded and decoded in quantum mechanical systems. There are many examples where encoding information in quantum states can be much more efficient than classical ones. For example, one can use the fact that an n-dimensional quantum system has an exponential description in order to "encode" 2^n classical bits in it, for example in

*Centrum Wiskunde Informitica, Amsterdam, The Netherlands.
Email: A.G.Chailloux@cwi.nl.

†Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris Diderot, Paris, France and Centre for Quantum Technologies, National University of Singapore, Singapore.
Email: jkeren@liafa.univ-paris-diderot.fr.

‡Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris Diderot, Paris, France.
Email: jamie.sikora@liafa.univ-paris-diderot.fr.

a quantum fingerprint state [BCWdW01]. However, quantum information does not always offer some advantage, since the uncertainty principle postulates that every time an external observer measures a quantum system, the state of the system collapses after the measurement and some information may become irretrievable. This intricate interplay between these two properties has been at the basis of some of the most fundamental results in quantum information, from quantum encodings, to non-locality, and to quantum cryptography.

Our goal is to study the relation between these areas and provide new insight on the power and limitations of quantum information, by looking at it through these various lenses. After describing in more detail the different concepts that we study, we prove some precise quantitative equivalences between them and provide a number of applications.

1.1 Quantum encodings and learning the XOR

One of the fundamental results in quantum information is Holevo's theorem [Hol73] which, in high level, says that if one wants to transmit classical information, then encoding the classical information into quantum bits is no more efficient than encoding it into classical bits. In other words, classical information cannot be compressed using quantum information. The same negative result holds for the weaker task that is referred to as Random Access Codes. Here, one is looking for an encoding of n classical bits into a quantum state, where each bit can be decoded with high probability from a single copy of the encoding (but not necessarily all of them at the same time). Again, quantum encodings are no more efficient than classical ones [Nay99].

However, the extraordinary power of quantum information has been proven in a variety of models: for example, in communication complexity, there is a number of distributed tasks, where quantum encodings are exponentially more efficient than classical ones [BCWdW01, BJK04, GKK$^+$08, RK11]. Moreover, it is possible to encode two classical bits in one quantum bit such that either bit can be correctly decoded with probability $\cos^2(\pi/8)$, see [BBBW83, ANTV99].

Let us focus on the following simple scenario: The quantum state ρ_{x_0,x_1} encodes two classical bits x_0 and x_1 that are drawn from some known distribution. Imagine there exists a decoding procedure (i.e. a quantum measurement) to decode x_0 that provides the correct answer with probability p_0 and a different decoding procedure that decodes x_1 with probability p_1. We would like to analyse the *average decoding probability*, i.e. the quantity $(p_0 + p_1)/2$.

One way to bound this quantity is through entropic uncertainty relations, which can provide upper bounds on this probability that depend on the decoding procedures but not on the encoding (see for example [OW10]). For example, if the first decoding procedure is a measurement in the computational basis and the second in the Hadamard basis, it is easy to see that no matter what quantum encoding we use, there is always some entropy in the distribution of outcomes of these two measurements. This, in turn, implies that the average decoding probability cannot be 1.

Here, we study the average decoding probability by relating it to the probability of decoding some other function $f(x_0, x_1)$ of the bits, for example the one that outputs both bits or their XOR. Classically, it is straightforward to relate the probability of decoding $f(x_0, x_1)$ to the probabilities of decoding each bit x_i. If one has some partial information about (x_0, x_1) then it is easy to find

the optimal guess for (x_0, x_1). However, the situation is more delicate in the quantum world. Suppose we try to determine $f(x_0, x_1)$ by decoding each bit x_i. Once the first bit is decoded, the encoding collapses to some eigenstate of the decoding operator, hence the probability of then correctly decoding the second bit may have changed. In other words, getting information about x_0 could destroy the information about x_1.

We provide new upper bounds on the average decoding probability of two classical bits that depend on the probability of correctly decoding both bits or the XOR of the two bits. We also extend these results to strings and discuss their relation to complementarity.

Theorem 1 (XOR learning lemmata) *Let $\{\rho_{x_0,x_1} : x_0, x_1\}$ be a quantum encoding of two classical bits (or bit strings) x_0, x_1 drawn from some known probability distribution. Denote the average decoding probability of x_0 and x_1 by $c := \frac{1}{2}\Pr[\text{learning } x_0] + \frac{1}{2}\Pr[\text{learning } x_1]$. Then*

1. $\Pr[\text{learning } x_0 \oplus x_1] \geq (2c-1)^2$ *when* $x_0, x_1 \in \{0,1\}$,
2. $\Pr[\text{learning } x_0 \oplus x_1] \geq c(2c-1)^2$, *if* $c \geq 1/2$, *when* $x_0, x_1 \in \{0,1\}^n$.
   In fact, $\Pr[\text{learning } (x_0, x_1)] \geq c(2c-1)^2$, *if* $c \geq 1/2$, *when* $x_0, x_1 \in \{0,1\}^n$.

The probability of learning a value is defined as the maximum over all decoding procedures of the probability that the output of the decoding procedure is equal to the correct value.

As a consequence of the previous theorem, in the case where the probability of learning $x_0 \oplus x_1$ is exactly $1/2$, i.e. the encoding reveals no information about the XOR, we have the following theorem.

Theorem 2 (Hidden XOR lemmata) *Let $\{\rho_{x_0,x_1} : x_0, x_1\}$ be a quantum encoding of two classical bits (or bit strings) x_0, x_1 drawn from some known probability distribution. If the encoding reveals no information about $x_0 \oplus x_1$, then*

1. $\frac{1}{2}\Pr[\text{learning } x_0] + \frac{1}{2}\Pr[\text{learning } x_1] \leq \cos^2(\pi/8)$ *when* $x_0, x_1 \in \{0,1\}$,
2. $\frac{1}{2}\Pr[\text{learning } x_0] + \frac{1}{2}\Pr[\text{learning } x_1] \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}$ *when* $x_0, x_1 \in \{0,1\}^n$.

In order to prove the above theorems, we study how the distribution of the measurement outcomes changes when we perform the two measurements sequentially on the same quantum state. We say that two measurements are perfectly complementary if after having performed the first measurement, no more information can be extracted by performing the second measurement on the post-measured state. On the other hand, they are non complementary if after measuring with one, the probabilities of the outcomes of the second are unaffected (which is the case for classical measurements). For example, the measurements on the computational and Hadamard bases are complementary while the measurements on different subsystems of a product state are non complementary. Our theorems provide a quantitive way of studying the notion of complementarity (see Appendix A). We also show how our lemmata are related to a number of fundamental properties of quantum information, including non-local games and quantum cryptographic primitives.

1.2 The CHSH game

The CHSH game is a well-known tool for studying quantum non-locality and the power of entanglement [CHSH69]. It is a game between Alice and Bob who initially share a quantum state and are not allowed to communicate any further. Alice receives a random $x \in \{0,1\}$ and outputs $a \in \{0,1\}$. Bob receives a random $y \in \{0,1\}$ and outputs $b \in \{0,1\}$. The value of the game, denoted $\omega^*(\mathrm{CHSH})$, is the maximum probability that $a \oplus b = yx$, which can be proven to be strictly higher than the value when Alice and Bob do not initially share any quantum state.

One can recast the CHSH game in the framework of quantum encodings and show that the value of the game is equal to Bob's average decoding probability depending on whether he receives $y = 0$ or $y = 1$. For example, once Alice receives x and measures to learn a, the post-measured state Bob has is an encoding of a and x. We can thus write the value of the game as

$$\Pr[\text{Bob receives } y = 0]\Pr[\text{Bob outputs } b = a] + \Pr[\text{Bob receives } y = 1]\Pr[\text{Bob outputs } b = a \oplus x]$$

which can be rewritten as

$$\frac{1}{2}\Pr[\text{Bob can learn } a] + \frac{1}{2}\Pr[\text{Bob can learn } a \oplus x].$$

Note also that the non-signalling condition of the CHSH game says that the probability that Bob can guess Alice's input is $1/2$ can be equivalently stated as the fact that the maximum probability of correctly decoding the XOR of a and $a \oplus x$ (the two bits Bob wishes to learn in this case) is $1/2$. With this perspective, we can see how the CHSH game is related to quantum encodings where the XOR is hidden.

In [OW10], they explore this idea further by providing some close relations between special types of uncertainty relations and the value of the CHSH game in quantum but also more general theories.

1.3 Oblivious transfer

Oblivious transfer is a fundamental cryptographic primitive, where Alice sends to Bob one of two bits (x_0, x_1) but is oblivious to the bit Bob receives. We wish to design protocols to accomplish the following three (conflicting) tasks: Alice cannot learn which bit is received by Bob, Bob cannot learn the XOR[1] of Alice's two bits, Bob learns the correct value when both parties are honest.

Let us define OT_p with cheating probabilities as follows (formal definitions of all primitives and games used in this paper can be found in Section 2):

- Alice outputs (z_0, z_1) and Bob outputs (b, w), where z_0, z_1, b are uniformly random bits and $w = z_b$ with probability p,

[1] Note that most definitions enforce the stronger condition on cheating Bob, that he has no (or very little) information about Alice's other bit (instead of the XOR of her bits). However, in the classical world, if Bob cannot guess the XOR then he does not know one of the two bits [DFSS06]. In the quantum world, we show that this definition of cheating Bob relates directly to the CHSH game.

- A_{OT} is the maximum probability Alice can guess b without being caught cheating,
- B_{OT} is the maximum probability Bob can guess $z_0 \oplus z_1$ without being caught cheating,
- A protocol is *secure* if $A_{\mathrm{OT}} = B_{\mathrm{OT}} = 1/2$ and *perfect* if $p = 1$.

Oblivious transfer was first introduced as a "multiplexing channel" by Wiesner [Wie83] although the cryptographic relevance was not known at the time. It was first used in a cryptographic sense by Rabin [Rab81] as a way to share secrets. Rabin's version of oblivious transfer was not exactly as described above, however it was shown to be equivalent by Crépeau [Cré87]. Oblivious transfer is a fundamental primitive because it can be used to construct arbitrary secure function evaluation protocols [Kil88].

There are many quantum protocols for variants of oblivious transfer [BBBW83], [DFSS08], [WST08], [Sch10], [Sik12], [CKS13]. In particular, [BBBW83] showed a secure protocol where Bob gets the correct value with probability $\cos^2(\pi/8)$. On the other hand, when Bob gets the correct value with probability 1, then Alice or Bob can cheat with probability 58.52%, independent of what function of (x_0, x_1) Bob wishes to learn [CKS13].

In this paper, we are using the stand-alone definition of oblivious transfer, which does not guarantee composability. This makes our lower bounds on the cheating probabilities stronger, and in addition, this definition highlights the relations between non-locality, cryptography, and quantum encodings.

To further discuss composability, let us consider a non-interactive OT_p protocol where Alice sends to Bob a quantum encoding and Bob can choose which bit to learn by measuring in a particular basis. Consider using such a protocol to accomplish the following cryptographic task, known as imperfect Rabin OT (the perfect version was introduced in [Rab81]), as follows:

- Alice and Bob use a non-interactive OT_p protocol so that Bob learns z_b with probability p.
- Alice sends to Bob a random bit c and outputs the value z_c. If $b = c$, Bob outputs z_c (with probability p). If $b \neq c$, he outputs $\#$.

We see that Bob need only delay his choice of b (and his measurement) to always learn z_c with probability p. If Bob was forced to measure at the end of the OT_p protocol, before learning c, then he would know z_c (with probability p) only if $c = b$. Therefore, the protocols we consider in this paper, even if secure and non-interactive, are not necessarily composable. It should be clear that our goal is to relate this cryptographic primitive to non-local games and the notion of complementarity of quantum measurements, and not to construct real-life security systems.

We now examine how the correctness is related to the security of oblivious transfer. In particular, we answer the question of whether it is possible to sacrifice a little security for the sake of gaining much correctness by showing a lower bound curve relating the three quantities p, A_{OT}, and B_{OT}.

Theorem 3 (Lower bound curve for imperfect oblivious transfer) *For any* OT_p *protocol, the correctness parameter* p *and cheating probabilities* A_{OT} *and* B_{OT} *satisfy*

$$p \leq A_{\mathrm{OT}} \left(\sqrt{B_{\mathrm{OT}}} + 1 \right).$$

When we set $A_{\mathrm{OT}} = B_{\mathrm{OT}} = 1/2$, we get that for secure protocols $p \leq \cos^2(\pi/8)$, which is attainable by the secure protocol mentioned above in [BBBW83]. Therefore, the curve contains the point corresponding to the largest correctness of a secure oblivious transfer protocol. However, not every point on this curve is optimal. If we set $p = 1$, i.e., the protocol is perfect, we get that $\max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\} \geq 56.98\%$. In fact, we prove a stronger lower bound of 59.9% as well as extend the bound of 58.52% to *oblivious string transfer*, denoted OT_p^n, which is the same as OT_p, except Alice outputs n-bit strings instead of single bits.

Theorem 4 (Security lower bounds on perfect oblivious transfers) *In any perfect* OT_1 *protocol, one party can cheat with probability at least* 59.9%*. Also, for any* $n \in \mathbb{N}$ *and any* OT_1^n *protocol, one party can cheat with probability at least* 58.52% *regardless of the function of Alice's two strings Bob wishes to learn.*

This shows that the security of perfect oblivious transfer cannot be amplified to get arbitrarily close to 50% without sacrificing some correctness. The proofs of the above two theorems are similar to the lower bound proof in [CKS13] and are detailed in Appendix B.

1.4 Equivalences between CHSH games and secure OT protocols

The learning and hiding lemmata appear to have strong connections with non-local games as well as cryptographic primitives. In Section 4, we make this explicit and prove (or in some cases reprove) some bounds for CHSH-type games as well as variations of quantum oblivious transfer. In fact, we prove two equivalences, each involving three different notions: quantum information theory, quantum games, and quantum cryptography. The first equivalence we prove involves quantum encodings hiding the XOR of two strings; the primitive OT_p^n; and the game CHSH_n, where Alice receives random $x \in \{0,1\}^n$ and outputs $a \in \{0,1\}^n$, Bob receives random *bit* $y \in \{0,1\}$ and outputs $b \in \{0,1\}^n$, and they win if $a_i \oplus b_i = y\, x_i$ for all $i \in \{1, \ldots, n\}$ (the XOR is bitwise and $y\, x_i$ is scalar multiplication). Formal definitions of the games and primitives can be found in Section 2.

Theorem 5 (Equivalence of secure $\mathrm{OT}_{\mathbf{p}}^{\mathbf{n}}$ and $\mathrm{CHSH}_{\mathbf{n}}$ strategies) *The following four statements are equivalent for every* $n \in \mathbb{N}$*:*

1. *There exists a set of quantum states* $\{\rho_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ *and a probability distribution* $\{\pi_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ *such that when given* ρ_{x_0,x_1} *with probability* π_{x_0,x_1}*:*

$$\Pr[\text{learning } x_0 \oplus x_1] = \frac{1}{2^n} \quad \text{and} \quad \frac{1}{2}\Pr[\text{learning } x_0] + \frac{1}{2}\Pr[\text{learning } x_1] = p;$$

2. *There exists a secure, non-interactive* OT_p^n *protocol;*

3. *There exists a secure* OT_p^n *protocol;*

4. *There exists a strategy for* CHSH_n *that succeeds with probability* p*.*

We also prove another equivalence between quantum encodings of n pairs of bits hiding each XOR; $\mathrm{OT}_p^{\otimes n}$, the n-fold parallel repetition of oblivious transfer; and $\mathrm{CHSH}^{\otimes n}$, the n-fold parallel repetition of CHSH. Again, p is the correctness parameter of the oblivious transfer protocol.

Theorem 6 (Equivalence of secure $\mathrm{OT}_{\mathbf{p}}^{\otimes \mathbf{n}}$ **and** $\mathrm{CHSH}^{\otimes \mathbf{n}}$**)** *The following four statements are equivalent for every* $n \in \mathbb{N}$*:*

1. *There exists a set of quantum states* $\{\rho_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ *and a probability distribution* $\{\pi_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ *such that when given* ρ_{x_0,x_1} *with probability* π_{x_0,x_1}*:*

$$\Pr[\text{learning } x_0 \oplus x_1] = \frac{1}{2^n} \quad \text{and} \quad \frac{1}{2^n} \sum_{c \in \{0,1\}^n} \Pr[\text{learning } x_c] = p,$$

   where x_c *is the string with* i*'th bit being the* i*'th bit of the string* x_{c_i}*;*

2. *There exists a secure, non-interactive* $\mathrm{OT}_p^{\otimes n}$ *protocol;*

3. *There exists a secure* $\mathrm{OT}_p^{\otimes n}$ *protocol;*

4. *There exists a strategy for* $\mathrm{CHSH}^{\otimes n}$ *that succeeds with probability* p*.*

Note that in our equivalences, apart from translating the learning probabilities, we conserve the notions of security/non-signalling/hidden XOR through the reductions and we also deal with the interactivity and aborting of oblivious transfer protocols.

In related work, Wolf and Wullschleger [WW05] showed that PR-Boxes, imaginary boxes that win the CHSH game with probability 1, are equivalent to perfect secure oblivious transfer. However, there is a timing issue as pointed out in [BCU$^+$05] that makes the OT non-composable. Our results also extend these connections to the quantum world.

1.5 Applications of the equivalences

Our equivalences provide new ways of looking at quantum cryptographic primitives, quantum non-local games, and quantum encodings. They also allow for interesting, or even surprising, consequences. One reason is that we can use previous results in one area to prove bounds in another. For example, instead of proving a bound directly for oblivious transfer, one could use a bound for CHSH to obtain a bound for oblivious transfer. Take for example the semidefinite programs used to show perfect parallel repetition of XOR games [CSUU08]. These seem to have no connections

with interactive oblivious transfer protocols, however they are intricately linked through our second equivalence result and therefore can be used to say something about oblivious transfer.

Using Theorem 2 and the equivalences in Theorem 5, we have an alternative proof of the optimality of CHSH and an upper bound on CHSH_n. We discuss the optimality of our bound on CHSH_n in Appendix D.

Corollary 1 (Bounds on CHSH and CHSH_n) *For any $n \in \mathbb{N}$, $\omega^*(\mathrm{CHSH}_n) \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}$. Furthermore, $\omega^*(\mathrm{CHSH}) \leq \cos^2(\pi/8)$, which is attainable by* [CHSH69].

Moreover, we have the following bounds on secure oblivious transfer.

Corollary 2 (Bounds on $\mathrm{OT}_{\mathbf{p}}^{\mathbf{n}}$ and $\mathrm{OT}_{\mathbf{p}}$) *For any $n \in \mathbb{N}$, the correctness of any secure OT_p^n protocol satisfies $p \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}$. Furthermore, the correctness of any secure oblivious transfer protocol OT_p must satisfy $p \leq \cos^2(\pi/8)$, which is attainable by* [BBBW83].

Using perfect parallel repetition of CHSH [CSUU08], we have the following corollary of Theorem 6.

Corollary 3 (Perfect parallel repetition of oblivious transfer) *For any $n \in \mathbb{N}$, the correctness of any secure $\mathrm{OT}_p^{\otimes n}$ protocol satisfies $p \leq (\cos^2(\pi/8))^n$, which is attainable by using n instances of a secure $\mathrm{OT}_{\cos^2(\pi/8)}$ protocol. That is, secure oblivious transfer admits perfect parallel repetition.*

On the other hand, we get another variation of the hiding lemma when the XOR of Alice's two strings are hidden.

Lemma 1 (Hidden XOR string lemma, version 2) *Let $\{\rho_{x_0,x_1} : x_0, x_1\}$ be a quantum encoding of two classical n-bit strings x_0, x_1 that are drawn from some known probability distribution. If the encoding reveals no information about $x_0 \oplus x_1$, then*

$$\frac{1}{2^n} \sum_{c \in \{0,1\}^n} \Pr[\text{learning } x_c] \leq \left(\cos^2(\pi/8)\right)^n.$$

2 Cryptographic primitives and quantum game definitions

We give formal definitions of the cryptographic primitives and quantum games used in this paper.

Definition 1 (Imperfect oblivious transfer) *A quantum oblivious transfer protocol with correctness p, denoted here as OT_p, is an interactive protocol, with no inputs, between Alice and Bob such that:*

- *Alice outputs two independent, uniformly random bits (z_0, z_1) or Abort and Bob outputs uniformly random bit b and another bit w or Abort.*

- *If Alice and Bob are honest, $w = z_b$ with probability p (for either value of b) and neither party aborts.*
- *If $p = 1$ we say the protocol is* perfect.

We say that the oblivious transfer protocol has cheating probabilities A_{OT} and B_{OT} where

- $A_{\mathrm{OT}} := \Pr[\text{Alice can learn } b \text{ without Bob aborting}]$,
- $B_{\mathrm{OT}} := \Pr[\text{Bob can learn } z_0 \oplus z_1 \text{ without Alice aborting}]$,
- *If $A_{\mathrm{OT}} = 1/2$ and $B_{\mathrm{OT}} = 1/2$ we say the protocol is* secure.

The choice to have the information as outputs instead of inputs is for convenience since Alice and Bob can always derandomize their outputs while retaining the same cheating probabilities (see [CKS13] for details).

Definition 2 (Imperfect oblivious string transfer) *A quantum oblivious string transfer protocol with correctness p, denoted here as OT_p^n, with cheating probabilities A_{OT^n} and B_{OT^n}, is defined analogously to an imperfect oblivious transfer protocol except z_0 and z_1 are n-bit strings. We say an OT_p^n protocol is secure if $A_{\mathrm{OT}^n} = 1/2$ and $B_{\mathrm{OT}^n} = 1/2^n$, noting that Bob wishes to learn $z_0 \oplus z_1$.*

Definition 3 (n-fold repetition of oblivious transfer) *A quantum n-fold repetition of oblivious transfer protocol with correctness p, denoted here as $\mathrm{OT}_p^{\otimes n}$, with cheating probabilities $A_{\mathrm{OT}^{\otimes n}}$ and $B_{\mathrm{OT}^{\otimes n}}$, is defined analogously to an imperfect oblivious string transfer protocol except b is an n-bit string (so z_b takes values from each of Alice's strings according to b). We say an $\mathrm{OT}_p^{\otimes n}$ protocol is secure if $A_{\mathrm{OT}^{\otimes n}} = 1/2^n$ and $B_{\mathrm{OT}^{\otimes n}} = 1/2^n$, noting that Bob wishes to learn $z_0 \oplus z_1$.*

Definition 4 (Imperfect coin flipping) *A quantum coin flipping protocol with correctness p, denoted here as CF_p, is an interactive protocol, with no inputs, between Alice and Bob such that:*

- *The protocol is aborted with probability $1 - p$ when Alice and Bob are honest.*
- *If the protocol is not aborted, then they both output a randomly generated bit c.*

We say that the coin flipping protocol has cheating probabilities A_{CF} and B_{CF} where

- $A_{\mathrm{CF}} := \max_{c \in \{0,1\}} \Pr[\text{Alice can force Bob to accept outcome } c]$,
- $B_{\mathrm{CF}} := \max_{c \in \{0,1\}} \Pr[\text{Bob can force Alice to accept outcome } c]$.

Definition 5 (Bit commitment) *A quantum bit commitment protocol, denoted here as BC, is an interactive protocol with no inputs, between Alice and Bob, with two phases:*

- *Commit phase: Bob chooses a random b and interacts with Alice to commit to b.*

- *Reveal phase: Alice and Bob interact to reveal b to Alice.*
- *If the parties are honest, Alice accepts the value of b and neither party aborts.*

We say that the bit commitment protocol has cheating probabilities A_{BC} and B_{BC} where

- $B_{\mathrm{BC}} := \sum_{b\in\{0,1\}} \frac{1}{2} \Pr[\text{Bob can force Alice to accept outcome } b]$,
- $A_{\mathrm{BC}} := \Pr[\text{Alice can learn } b \text{ after commit phase}]$.

Note that the roles of Alice and Bob are usually inverted, however this definition is more convenient for the analysis in this paper.

Definition 6 (CHSH_n game) *The CHSH_n game is a game between Alice and Bob where:*

- *Alice and Bob are allowed to create and share an entangled state $|\psi\rangle$ before the game starts. Once the game starts, there is no further communication between Alice and Bob.*
- *Alice receives a random $x \in \{0,1\}^n$ and Bob receives a random $y \in \{0,1\}$.*
- *Alice outputs $a \in \{0,1\}^n$ and Bob outputs $b \in \{0,1\}^n$.*
- *Alice and Bob win if $a_i \oplus b_i = y\, x_i$, for all $i \in \{1,\ldots,n\}$.*

The value of the game, denoted here as $\omega^*(\mathrm{CHSH}_n)$, is the maximum probability which Alice and Bob can win.

The CHSH game is the special case when $n = 1$ (we omit the subscript 1 in this case).

Definition 7 (n-fold repetition of CHSH) *An n-fold repetition of CHSH, denoted here as $\mathrm{CHSH}^{\otimes n}$, is a game between Alice and Bob where:*

- *Alice and Bob are allowed to create and share an entangled state $|\psi\rangle$ before the game starts. Once the game starts, there is no further communication between Alice and Bob.*
- *Alice receives a random $x \in \{0,1\}^n$ and Bob receives a random $y \in \{0,1\}^n$.*
- *Alice outputs $a \in \{0,1\}^n$ and Bob outputs $b \in \{0,1\}^n$.*
- *Alice and Bob win if $a_i \oplus b_i = x_i\, y_i$, for all $i \in \{1,\ldots,n\}$.*

The value of the game, denoted here as $\omega^*(\mathrm{CHSH}^{\otimes n})$, is the maximum probability which Alice and Bob can win.

3 Learning and hiding lemmata

3.1 Proofs of theorems

In order to prove Theorem 1 and Theorem 2, we need the following claim about performing two projective measurements in sequence that could be of independent interest.

Claim 1 *Let $|\psi\rangle$ be a pure state and $\{C, I-C\}$ and $\{D, I-D\}$ be two projective measurements such that*

$$\cos^2(\alpha) := \|C|\psi\rangle\|_2^2 \geq \frac{1}{2} \quad \text{and} \quad \cos^2(\beta) := \|D|\psi\rangle\|_2^2 \geq \frac{1}{2}.$$

Then we have

$$\cos^2(\alpha-\beta) \geq \|CD|\psi\rangle\|_2^2 + \|(I-C)(I-D)|\psi\rangle\|_2^2 \geq \cos^2(\alpha+\beta).$$

Proof We first prove the lower bound. Define the following states

$$|X\rangle := \frac{C|\psi\rangle}{\|C|\psi\rangle\|_2}, |X'\rangle := \frac{(I-C)|\psi\rangle}{\|(I-C)|\psi\rangle\|_2}, |Y\rangle := \frac{D|\psi\rangle}{\|D|\psi\rangle\|_2}, |Y'\rangle := \frac{(I-D)|\psi\rangle}{\|(I-D)|\psi\rangle\|_2}.$$

We have $|\psi\rangle = \cos(\alpha)|X\rangle + \sin(\alpha)|X'\rangle = \cos(\beta)|Y\rangle + \sin(\beta)|Y'\rangle$. Since $|X\rangle$ is an eigenvector of C, we can write $C = |X\rangle\langle X| + \Pi_C$ and similarly we can write $I - C = |X'\rangle\langle X'| + \Pi_{C'}$, such that

$$\langle \Pi_C, |X\rangle\langle X| \rangle = \langle \Pi_{C'}, |X\rangle\langle X| \rangle = \langle \Pi_C, |X'\rangle\langle X'| \rangle = \langle \Pi_{C'}, |X'\rangle\langle X'| \rangle = 0.$$

We now write

$$|Y\rangle = \gamma_0|X\rangle + \gamma_1|X'\rangle + \gamma_2|Z\rangle$$

where $\||Z\rangle\|_2 = 1$, $\langle X|Z\rangle = \langle X'|Z\rangle = 0$ and $|\gamma_0| = \sqrt{x_0}$, $|\gamma_1| = \sqrt{x_1}$, and $|\gamma_2| = \sqrt{x_2}$ for some $x_0, x_1, x_2 \in [0,1]$. Using this expression for $|Y\rangle$, we have

$$\|CD|\psi\rangle\|_2^2 = \cos^2(\beta)\,\|C|Y\rangle\|_2^2 = \cos^2(\beta)\left(x_0 + x_2\,\|\Pi_C|Z\rangle\|_2^2\right).$$

Since $|\psi\rangle = \cos(\alpha)|X\rangle + \sin(\alpha)|X'\rangle = \cos(\beta)|Y\rangle + \sin(\beta)|Y'\rangle$, we can write

$$|Y'\rangle = \gamma_0'|X\rangle + \gamma_1'|X'\rangle + \gamma_2'|Z\rangle$$

with $|\gamma_0'| = \sqrt{x_0'}$, $|\gamma_1'| = \sqrt{x_1'}$, and $|\gamma_2'| = \sqrt{x_2'}$ for some $x_0', x_1', x_2' \in [0,1]$. Using this expression for $|Y'\rangle$, we have

$$\|(1-C)(1-D)|\psi\rangle\|_2^2 = \sin^2(\beta)\left\|(1-C)|Y'\rangle\right\|_2^2 = \sin^2(\beta)\left(x_1' + x_2'\,\|\Pi_{C'}|Z\rangle\|^2\right).$$

Notice that

$$1 = \|C|Z\rangle\|_2^2 + \|(I-C)|Z\rangle\|_2^2 = \|\Pi_C|Z\rangle\|_2^2 + \|\Pi_{C'}|Z\rangle\|_2^2.$$

We define $A := \|\Pi_C|Z\rangle\|_2^2 = 1 - \|\Pi_{C'}|Z\rangle\|_2^2$. This gives us

$$\begin{aligned}
& \|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \\
= \;& \cos^2(\beta)\left(x_0 + x_2\|\Pi_C|Z\rangle\|_2^2\right) + \sin^2(\beta)\left(x_1' + x_2'\|\Pi_{C'}|Z\rangle\|_2^2\right) \\
= \;& \cos^2(\beta)\left(x_0 + x_2 A\right) + \sin^2(\beta)\left(x_1' + x_2'(1-A)\right) \\
= \;& \cos^2(\beta)x_0 + \sin^2(\beta)\left(x_1' + x_2'\right) + A\left(\cos^2(\beta)x_2 - \sin^2(\beta)x_2'\right) \\
= \;& \cos^2(\beta)x_0 + \sin^2(\beta)\left(1 - x_0'\right) + A\left(\cos^2(\beta)x_2 - \sin^2(\beta)x_2'\right). \qquad (1)
\end{aligned}$$

Define $A(\rho,\sigma) := \arccos F(\rho,\sigma)$ to be the angle between two states ρ and σ, which is a metric (see p. 413 in [NC00]). Since $\langle Y|Y'\rangle = 0$, we have

$$A(|Y'\rangle, |X\rangle) \geq \pi/2 - A(|X\rangle, |Y\rangle).$$

This implies that

$$\sqrt{x_0'} = \cos\left(\arccos|\langle Y'|X\rangle|\right) \leq \cos\left(\pi/2 - \arccos\sqrt{x_0}\right) = \sin\left(\arccos\sqrt{x_0}\right) = \sqrt{1-x_0}.$$

This yields $x_0' \leq 1 - x_0$. Also, notice that $\langle\psi|Z\rangle = 0$, which implies that

$$\begin{aligned}
& \langle Z|\left(\cos(\beta)|Y\rangle + \sin(\beta)|Y'\rangle\right) = 0 \\
\iff \;& \cos^2(\beta)|\langle Z|Y\rangle|^2 = \sin^2(\beta)|\langle Z|Y'\rangle|^2 \\
\iff \;& \cos^2(\beta)x_2 = \sin^2(\beta)x_2'.
\end{aligned}$$

This gives us the bound

$$\|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \geq x_0. \qquad (2)$$

To conclude, we have

$$\arccos(\sqrt{x_0}) = A(|X\rangle, |Y\rangle) \leq A(|X\rangle, |\psi\rangle) + A(|\psi\rangle, |Y\rangle) \leq \alpha + \beta,$$

yielding $x_0 \geq \cos^2(\alpha+\beta)$ which concludes the proof of the lower bound.

For the upper bound, we have $x_0' \leq 1 - x_0$ and $\cos^2(\beta)x_2 = \sin^2(\beta)x_2'$, hence,

$$\|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \leq 1 - x_0',$$

from (1). We now show $1 - x_0' \leq \cos^2(\beta-\alpha)$. Since $\sqrt{x_0'} = |\langle Y'|X\rangle|$, we have

$$\arccos\left(\sqrt{x_0'}\right) = A(|Y'\rangle, |X\rangle) \leq A(|X\rangle, |\psi\rangle) + A(|Y'\rangle, |\psi\rangle) = \pi/2 - (\beta - \alpha).$$

so

$$\sqrt{x_0'} \geq \cos(\pi/2 - (\beta-\alpha)) = \sin(\beta-\alpha) \implies 1 - x_0' \leq \cos^2(\beta-\alpha),$$

as desired. □

Proof of Theorem 1 The proof of the first statement in the theorem relies on the following decoding strategy: First, we apply the decoding procedure for learning the first bit and then we apply the second decoding procedure on the post-measurement state. The probability of decoding the XOR is the probability that both decoding procedures succeed or they both fail.

We prove the theorem using the following (equivalent) setting. We suppose two parties, Alice and Bob, share a joint pure state $|\Omega\rangle_{\mathcal{AB}}$ such that Alice performs a projective measurement $M = \{M_{x_0,x_1}\}_{x_0,x_1\in\{0,1\}}$ on $\mathcal{A}$ to determine x_0 and x_1 and the post-measured state is Bob's encoding of x_0 and x_1. Let p_i be the maximum probability that Bob can learn bit x_i, for $i \in \{0,1\}$. We note that without loss of generality, Bob can perform a projective measurement to guess the value of x_i with maximum probability [NC00]. Let $P = \{P_0, P_1\}$ be Bob's projective measurement that allows him to guess x_0 with probability $p_0 = \cos^2(\alpha) \geq \frac{1}{2}$ and $Q = \{Q_0, Q_1\}$ be Bob's projective measurement that allows him to guess x_1 with probability $p_1 = \cos^2(\beta) \geq \frac{1}{2}$ (these measurements are on $\mathcal{B}$ only). Consider the following projections (on $\mathcal{A} \otimes \mathcal{B}$):

$$C = \sum_{x_0,x_1} M_{x_0,x_1} \otimes P_{x_0} \quad \text{and} \quad D = \sum_{x_0,x_1} M_{x_0,x_1} \otimes Q_{x_1}.$$

C (resp. D) is the projection on the subspace where Bob guesses correctly x_0 (resp. x_1) after applying P (resp. Q). Consider the strategy where Bob applies the two measurements P and Q one after the other to learn (x_0, x_1), from which he can calculate $x_0 \oplus x_1$. If both guesses are correct or if both guesses are incorrect then his guess for $x_0 \oplus x_1$ is correct.

Let Bob perform the following projective measurement to learn both bits

$$R = \{R_{x_0,x_1} := Q_{x_1} P_{x_0} Q_{x_1}\}_{x_0,x_1\in\{0,1\}}.$$

The measurement where Bob guesses both bits correctly when applying R is

$$E = \sum_{x_0,x_1} M_{x_0,x_1} \otimes R_{x_0,x_1} = DCD$$

with outcome probability $\langle\Omega|E|\Omega\rangle = \|CD|\Omega\rangle\|_2^2$. The measurement where Bob guesses both bits incorrectly when applying R is

$$F = \sum_{x_0,x_1} M_{x_0,x_1} \otimes R_{\bar{x_0},\bar{x_1}} = (I-D)(I-C)(I-D)$$

with outcome probability $\langle\Omega|F|\Omega\rangle = \|(I-C)(I-D)|\Omega\rangle\|_2^2$. With this strategy, Bob can guess $x_0 \oplus x_1$ with probability

$$||CD|\Omega\rangle||_2^2 + ||(I-C)(I-D)|\Omega\rangle||_2^2 \geq \cos^2(\alpha+\beta)$$

by Claim 1. Note that

$$c := \frac{p_0+p_1}{2} = \frac{\cos^2(\alpha)+\cos^2(\beta)}{2} \geq \frac{1}{2}$$

and by Claim 3 (in Appendix C), we have $\cos(\alpha+\beta) \geq \cos^2(\alpha) + \cos^2(\beta) - 1$. From this, we conclude that

$$\Pr[\text{Bob can learn } x_0 \oplus x_1] \geq \cos^2(\alpha+\beta) \geq (2c-1)^2.$$

For the second statement, ideally, we would like to extend our proof approach from bits to strings, but unfortunately this statement is not true anymore if x_0 and x_1 are strings. Instead, the analysis in [CKS13] can be generalized to strings to show

$$\Pr[\text{learning } (x_0, x_1)] \geq \left(\frac{\cos^2(\alpha) + \cos^2(\beta)}{2}\right) \cos^2(\alpha+\beta).$$

If $c \geq 1/2$, then by Claim 3 (in Appendix C), we have $\Pr[\text{learning } (x_0, x_1)] \geq c(2c-1)^2$. The statement about the XOR follows directly from the above statement. □

Proof of Theorem 2 By rearranging the XOR learning lemma for bits, we have

$$\frac{1}{2}\Pr[\text{learning } x_0] + \frac{1}{2}\Pr[\text{learning } x_1] \leq \frac{1}{2} + \frac{1}{2}\sqrt{\Pr[\text{learning } x_0 \oplus x_1]}.$$

Setting $\Pr[\text{learning } x_0 \oplus x_1] = 1/2$ yields the first statement of the theorem.

For the string version, we know that if the encoding reveals no information about $x_0 \oplus x_1$, then $\Pr[\text{learning } x_0 \oplus x_1] = \frac{1}{2^n}$. If $c := \frac{1}{2}\Pr[\text{learning } x_0] + \frac{1}{2}\Pr[\text{learning } x_1] \leq 1/2$, the theorem statement is clearly true. If $c \geq 1/2$, we get $\Pr[\text{Bob guesses } x_0 \oplus x_1] \geq c(2c-1)^2$ from Theorem 1. This yields

$$\frac{1}{2^n} = \Pr[\text{learning } x_0 \oplus x_1] \geq c(2c-1)^2 \geq \frac{1}{2}(2c-1)^2$$

which implies $c \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}$, as desired. □

Note that this bound for strings is not tight. In particular, for $n = 1$, this bound gives us $c \leq 1$ instead of $\cos^2(\pi/8) \simeq 0.854$. However, the probability goes exponentially fast to $1/2$ as n grows.

3.2 Applications

Using Theorem 1 and Theorem 2, we prove some new lower bounds for oblivious transfer. We first prove Theorem 3 by showing how to construct an imperfect coin flipping protocol from an imperfect oblivious transfer protocol.

Protocol 1 ($\mathrm{CF}_{\mathbf{p}}$ from $\mathrm{OT}_{\mathbf{p}}$)

1. *Alice and Bob perform the OT_p protocol so they have outputs (z_0, z_1) and (b, w) respectively.*
2. *If no one aborted, then Alice sends randomly chosen $d \in_R \{0,1\}$ to Bob.*
3. *Bob sends b and w to Alice.*

4. *If z_b from Bob is inconsistent with Alice's bits then Alice aborts. Otherwise, they both output $c = b \oplus d$.*

We see that this is a CF_p protocol since when both players are honest, there is a $1-p$ chance of aborting (from Alice's side), and otherwise the outcome is random.

Using our XOR learning lemma for bits, and an analysis similar to the one in [CKS13], we can show that

$$A_{\mathrm{OT}} = A_{\mathrm{CF}} \quad \text{and} \quad \frac{\sqrt{B_{\mathrm{OT}}}+1}{2} \geq B_{\mathrm{CF}}.$$

Kitaev's lower bound for coin flipping [Kit03] states that

$$A_{\mathrm{CF}} B_{\mathrm{CF}} \geq \Pr[\text{Alice and Bob honestly output } 0].$$

In the case of imperfect coin flipping, we have that Alice and Bob both output either bit with probability $p/2$ (since the protocol is aborted with probability $1-p$). Therefore, we have

$$A_{\mathrm{OT}} \frac{\sqrt{B_{\mathrm{OT}}}+1}{2} \geq A_{\mathrm{CF}} B_{\mathrm{CF}} \geq \frac{p}{2} \implies A_{\mathrm{OT}} \left(\sqrt{B_{\mathrm{OT}}}+1\right) \geq p,$$

proving Theorem 3.

In Appendix B, we construct a bit commitment protocol from an oblivious transfer protocol and by our XOR learning lemmata and the bit commitment lower bounds in [CK11] we prove the stronger lower bounds in Theorem 4.

4 Equivalences of secure oblivious transfer and CHSH

We give four reductions in order to prove Theorem 5, the reductions to prove Theorem 6 follow similarly. We show the reduction from hidden XOR to secure, non-interactive oblivious string transfer $(1. \implies 2.)$; from secure, non-interactive oblivious string transfer to CHSH_n strategies $(2. \implies 4.)$; from secure oblivious string transfer to hidden XOR $(3. \implies 1.)$; and from CHSH_n to hidden XOR $(4. \implies 1.)$. Since $(2. \implies 3.)$ is obvious, we have $(1. \implies 2. \implies 3., 4. \implies 1.)$ allowing us to conclude all four statements are equivalent.

Hidden XOR to secure, non-interactive $\mathrm{OT}^{\mathbf{n}}_{\mathbf{p}}$ $(\mathbf{1}. \implies \mathbf{2}.)$: Let $\{\rho_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ be a set of quantum states and $\{\pi_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ be a probability distribution satisfying the properties of statement 1 of Theorem 5. Alice chooses x_0, x_1 with probability π_{x_0,x_1} and sends ρ_{x_0,x_1} to Bob. Alice outputs

$$(z_0, z_1) := ((1-a)x_0 + ax_1 + d_1, (1-a)x_1 + ax_0 + d_2)$$

where a is a randomly chosen bit and d_1, d_2 are independent randomly chosen bit strings. She sends a, d_1, d_2 to Bob. The first bit randomizes the success probabilities for Bob (so he has an

equal chance of learning z_0 as for z_1) and the d_1, d_2 bit strings ensure that Alice's outcomes are random. Bob picks a uniformly random bit b and measures to learn z_b depending on a, d_1, d_2 from Alice. In particular, we have

$$\begin{aligned}\Pr[\text{Bob learns } z_b] &= \frac{1}{2}\Pr[\text{Bob learns } z_b | a = 0] + \frac{1}{2}\Pr[\text{Bob learns } z_{\bar{b}} | a = 1] \\ &= \frac{1}{2}\Pr[\text{Bob learns } x_0] + \frac{1}{2}\Pr[\text{Bob learns } x_1] \\ &= p,\end{aligned}$$

for $b \in \{0, 1\}$. Note that $z_0 \oplus z_1 = x_0 \oplus x_1 \oplus d_1 \oplus d_2$ is hidden from Bob and Alice cannot learn b, thus this protocol is secure.

Secure, non-interactive $\mathrm{OT}^{\mathbf{n}}_{\mathbf{p}}$ to $\mathrm{CHSH}_{\mathbf{n}}$ strategies ($\mathbf{2}. \implies \mathbf{4}.$): Suppose there is a secure, non-interactive OT^n_p protocol with correctness p. Without loss of generality,[2] Alice and Bob share the following classical-quantum state

$$\sum_{z_0, z_1 \in \{0,1\}^n} \frac{1}{2^{2n}} |z_0, z_1\rangle\langle z_0, z_1| \otimes \rho_{z_0, z_1},$$

for some quantum states ρ_{z_0,z_1} that are in Bob's private space $\mathcal{B}$. Since Alice has no information about b, the state sent by her is independent of b, hence Bob can use this state to decode either of Alice's strings. Let $\{M^0_{z_0}\}_{z_0 \in \{0,1\}^n}$ be Bob's measurement to learn Alice's first string and let $\{M^1_{z_1}\}_{z_1 \in \{0,1\}^n}$ be his measurement to learn Alice's second string. Since Bob can learn Alice's string with probability p, we have

$$p = \Pr[\text{Bob learns } z_0] = \sum_{z_0, z_1 \in \{0,1\}^n} \frac{1}{2^{2n}} \langle M^0_{z_0}, \rho_{z_0, z_1} \rangle \tag{3}$$

$$p = \Pr[\text{Bob learns } z_1] = \sum_{z_0, z_1 \in \{0,1\}^n} \frac{1}{2^{2n}} \langle M^1_{z_1}, \rho_{z_0, z_1} \rangle. \tag{4}$$

Now consider any purifications $|\psi_{z_0,z_1}\rangle \in \mathcal{A} \otimes \mathcal{B}$ of ρ_{z_0,z_1} where $\mathcal{A}$ is a space controlled by Alice. Let us define

$$|\Omega\rangle := \sum_{z_0, z_1 \in \{0,1\}^n} \frac{1}{2^n} |z_0 \oplus z_1\rangle_{\mathcal{A}_1} |z_0\rangle_{\mathcal{A}_2} |z_1\rangle_{\mathcal{A}_3} |\psi_{z_0,z_1}\rangle_{\mathcal{A}\mathcal{B}},$$

$|\Omega_x\rangle$ to be the post-measured state assuming Alice measured $\mathcal{A}_1$ to get x, and let Bob's reduced state on $\mathcal{B}$ be $\rho_x := \mathrm{Tr}_{\mathcal{A}_2\mathcal{A}_3\mathcal{A}} |\Omega_x\rangle\langle\Omega_x|$. We have that $\rho_x = \rho_0$ for all $x \in \{0,1\}^n$ since Bob has no information about $z_0 \oplus z_1$. By Uhlmann's theorem, we have that for all $x \in \{0,1\}^n$, there exists a unitary U_x acting on $\mathcal{A}_2 \otimes \mathcal{A}_3 \otimes \mathcal{A}$ such that $(U_x \otimes I_{\mathcal{B}})|\Omega_x\rangle = |\Omega_0\rangle$. We can now define the strategy for Alice and Bob to win the CHSH_n game with probability p:

[2] For our purposes, we can assume Alice discards her quantum state except for the registers containing her values for z_0 and z_1.

- Alice and Bob share the state $|\Omega_0\rangle$ and receive random $x \in \{0,1\}^n$ and $y \in \{0,1\}$, respectively.
- Alice applies $(U_x)^\dagger$ such that Alice and Bob share the state $|\Omega_x\rangle$. She measures the space $\mathcal{A}_2$ in the computational basis to get her outcome a.
- Bob applies the measurement $\{M_b^y\}_{b\in\{0,1\}^n}$ on his space $\mathcal{B}$ to determine his outcome b.

We now analyze this strategy. Conditioned on Alice receiving x and outputting a, Bob has the state $\mathrm{Tr}_{\mathcal{A}}|\psi_{a,x\oplus a}\rangle\langle\psi_{a,x\oplus a}| = \rho_{a,x\oplus a}$. If Bob gets $y=0$, he must output $b=a$. If Bob gets $y=1$, he must output $b = a\oplus x$. The probability they win the CHSH_n game with this strategy is

$$\begin{aligned} & \frac{1}{2}\Pr[\text{Bob learns } a] + \frac{1}{2}\Pr[\text{Bob learns } x\oplus a] \\ = \; & \frac{1}{2}\sum_{x,a\in\{0,1\}^n} \frac{1}{2^{2n}}\langle M_a^0, \rho_{a,x\oplus a}\rangle + \frac{1}{2}\sum_{x,a\in\{0,1\}^n}\frac{1}{2^{2n}}\langle M_{x\oplus a}^1, \rho_{a,x\oplus a}\rangle \\ = \; & p, \end{aligned}$$

from Equations (3) and (4).

Secure, interactive $\mathrm{OT}_{\mathbf{p}}^{\mathbf{n}}$ to hidden XOR ($\mathbf{3.} \implies \mathbf{1.}$): Let $|\Omega\rangle_{\mathcal{AB}}$ be the final joint state of the interactive OT_p^n protocol when Alice and Bob are honest. Suppose Alice measures to learn (z_0, z_1) which are both distributed uniformly. Let ρ_{z_0,z_1} be Bob's post-measured state. We now argue $\{\rho_{z_0,z_1} : z_0, z_1\}$ and π being the uniform probability distribution satisfy the hidden XOR condition. Since Alice does not abort because both parties have been honest, and the protocol is secure, we know the XOR is hidden from Bob. It now suffices to describe a decoding procedure to learn each z_c, for $c \in \{0,1\}$, with probability p.

We may assume Bob measures his part of the state $|\Omega\rangle_{\mathcal{AB}}$ (instead of decoding ρ_{z_0,z_1}) since it does not matter if Alice measures before or after Bob. Suppose $|\Omega_b\rangle_{\mathcal{AB}}$ is the post-measured joint state when Bob partially measures $|\Omega\rangle_{\mathcal{AB}}$ to obtain his index b. Since Bob will not abort at this stage and the protocol is secure, we know b is hidden from Alice. Again, by Uhlmann's theorem, we know that Bob can transform $|\Omega_0\rangle$ to $|\Omega_1\rangle$ and vice versa via a unitary acting on $\mathcal{B}$. Hence Bob can measure $|\Omega\rangle_{\mathcal{AB}}$ to learn b and collapse the state to $|\Omega_b\rangle$ and then apply the unitary mapping $|\Omega_b\rangle$ to $|\Omega_c\rangle$. He then uses the decoding procedure of the OT_p^n protocol to learn z_c with probability p.

$\mathrm{CHSH}_{\mathbf{n}}$ strategies to hidden XOR ($\mathbf{4.} \implies \mathbf{1.}$): Let $|\Omega\rangle_{\mathcal{AB}}$ be the state that Alice and Bob share before receiving x and y in a CHSH_n game strategy that succeeds with probability p. Suppose Alice measures to learn a (conditioned on x). Let $\rho_{a,x}$ be Bob's post-measured state which occurs with probability $\pi_{a,x}$. We define the necessary states and probabilities by relabelling $a \to x_0$ and $x\oplus a \to x_1$. Then, Bob has no information about $x_0 \oplus x_1 = a \oplus (x\oplus a) = x$ from non-signalling,

and

$$\frac{1}{2}\Pr[\text{Bob learns } x_0] + \frac{1}{2}\Pr[\text{Bob learns } x_1] = \frac{1}{2}\Pr[\text{Bob learns } a] + \frac{1}{2}\Pr[\text{Bob learns } x \oplus a] = p.$$

This concludes the proof of Theorem 5.

4.1 Applications of equivalences

As we have discussed in the introduction, our equivalences allow us to use results from one area to prove new results in another area. More specifically, using our Hidden XOR lemmata, we provide an alternative proof of the optimality of CHSH and an upper bound on CHSH_n (Corollary 1) and similar bounds for oblivious transfer (Corollary 2). In addition, using known results about the CHSH game, we prove an alternative Hidden XOR lemma for n pairs of bits and a parallel repetition result for secure oblivious transfer (Lemma 1 and Corollary 3).

Acknowledgements

Supported by ANR under the project ANR-09-JCJC-0067-01 and FP7 FET-Open project QCS.

References

[ANTV99] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 376 – 383, 1999.

[BBBW83] C. Bennett, G. Brassard, S. Breidbard, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology CRYPTO 1982*, pages 267–275, 1983.

[BCS12] H. Buhrman, M. Christandl, and C. Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Physical Review Letters*, 109(16):160501, 2012.

[BCU+05] H. Buhrman, M. Christandl, F. Unger, S. Wehner, and A. Winter. Implications of superstrong nonlocality for cryptography. In *Proceedings of the Royal Society A*, volume 462, pages 1919–1932, 2005.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.

[BJK04] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of 36th ACM STOC*, pages 128–137, 2004.

[CHSH69] J. Clauser, M. Horne, A. Shimony, and R. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[CK09] A. Chailloux and I. Kerenidis. Optimal quantum strong coin flipping. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:527–533, 2009.

[CK11] A. Chailloux and I. Kerenidis. Optimal bounds for quantum bit commitment. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 354–362. IEEE Computer Society Press, October 2011.

[CKS13] A. Chailloux, I. Kerenidis, and J. Sikora. Lower bounds for quantum oblivious transfer. *Quantum Information and Computation*, 13(1&2):158–177, 2013.

[Col07] R. Colbeck. The impossibility of secure two-party classical computation. *Phys. Rev. A*, 76:062308, 2007.

[Cré87] C. Crépeau. Equivalence between two flavours of oblivious transfers. In *CRYPTO 1987*, pages 350–354, 1987.

[CSUU08] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theroem for quantum XOR proof systems. *Computational Complexity*, 17(2):282–299, 2008.

[DFSS06] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Oblivious transfer and linear functions. In *Advances in Cryptology - CRYPTO 2006*, pages 427–444, 2006.

[DFSS08] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. *SIAM J. Comput.*, 37(6):1865–1890, 2008.

[EGL82] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. In *CRYPTO 1982*, pages 205–210, 1982.

[GKK$^+$08] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput.*, 38(5):1695–1708, 2008.

[Hol73] A. Holevo. Some estimates of the information transmitted by quantum communication channels. *Problemy Peredachi Informatsii*, 9:3–11, 1973.

[JRS02] R. Jain, J. Radhakrishnan, and P. Sen. A theorem about relative entropy of quantum states with an application to privacy in quantum communication. In *Proceedings of 43rd IEEE Symposium on Foundations of Computer Science*, 2002.

[Kil88] J. Kilian. Founding crytpography on oblivious transfer. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 20–31, New York, NY, USA, 1988. ACM Press.

[Kit03] A. Kitaev. Quantum coin-flipping. Presentation at the 6th workshop on quantum information processing (QIP 2003), 2003.

[KRT10] J. Kempe, O. Regev, and B. Toner. Unique games with entangled provers are easy. *SIAM Journal on Computing*, 39(7):3207–3229, 2010.

[Lo97] H.-K. Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56(2):1154–1162, 1997.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. *Proceedings of 40th IEEE Symposium on Foundations of Computer Science*, 0:369–376, 1999.

[NC00] M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[OW10] J. Oppenheim and S. Wehner. The uncertainty principle determines the non-locality of quantum mechanics. *Science*, 330:6007:1072–1074, 2010.

[Rab81] M. Rabin. How to exchange secrets by oblivious transfer. In *Technical Report TR-81, Aiken Computation Laboratory, Harvard University*, 1981.

[RK11] O. Regev and B. Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In *STOC*, pages 31–40, 2011.

[Sch10] C. Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Phys. Rev. A*, 82:032308, 2010.

[Sik12] J. Sikora. On the existence of loss-tolerant quantum oblivious transfer protocols. *Quantum Information and Computation*, 12(7&8):609–619, 2012.

[SSS09] L. Salvail, C. Schaffner, and M. Sotakova. On the power of two-party quantum cryptography. In *ASIACRYPT 2009*, 2009.

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[WST08] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100(22):220502, 2008.

[WW05] S. Wolf and J. Wullschleger. Oblivious transfer and quantum non-locality. In *Proceedings of International Symposium on Information Theory*, pages 1745 –1748, 2005.

[Yao95] A. Yao. Security of quantum protocols against coherent measurements. In *Proceedings of 26th Annual ACM Symposium on the Theory of Computing*, pages 67–75. ACM, 1995.

A Bounds on the complementarity of measurements

Let us assume for a quantum state $|\psi\rangle$ and two measurements $\{C, I-C\}$ and $\{D, I-D\}$, that measuring the state $|\psi\rangle$ with the measurement $\{C, I-C\}$ yields the "correct" outcome C with probability $\cos^2(\alpha)$ and the "wrong" outcome $I-C$ with probability $\sin^2(\alpha)$; and similarly, measuring the state $|\psi\rangle$ with the measurement $\{D, I-D\}$ yields the "correct" outcome D with probability $\cos^2(\beta)$ and the "wrong" outcome $I-D$ with probability $\sin^2(\beta)$.

We would like to study how the effect of performing the first measurement changes the information we can extract through the second measurement. Two measurements are perfectly complementary, if after having performed the first measurement, no more information can be extracted by performing the second measurement on the measured state. On the other hand, they are non complementary if after measuring with one, the probabilities of the outcomes of the second are unaffected (which is the case for classical measurements).

We provide a quantitative analysis for the case where the information is correctly decoded when both measurements output the correct outcome or both output the wrong outcome (as for example, in the case of trying to learn the XOR of two bits by decoding one after the other). Let us define Γ as the following measure

$$\Gamma = \|CD|\psi\rangle\|_2^2 + \|(I-C)(I-D)|\psi\rangle\|_2^2 - \|C|\psi\rangle\|_2^2 \|D|\psi\rangle\|_2^2 - \|(I-C)|\psi\rangle\|_2^2 \|(I-D)|\psi\rangle\|_2^2 .$$

In the case of non complementary measurements, $\Gamma = 0$. By Claim 1, we have

$$|\Gamma| \leq \frac{1}{2}\sin(2\beta)\sin(2\alpha). \tag{5}$$

Note that Γ can take both positive and negative values, since the act of performing the second measurement on the post-measured state can increase or decrease the probability of correctly decoding. The inequality (5) can be tight, since when $C = D$, we have $\Gamma = \frac{1}{2}\sin(2\beta)\sin(2\alpha)$ and when $C = I - D$, we have $\Gamma = -\frac{1}{2}\sin(2\beta)\sin(2\alpha)$.

B Lower bounds on the security of perfect oblivious transfers

We now define a bit commitment protocol where the commit phase is a perfect oblivious transfer protocol and the reveal phase is classical.

Protocol 2 (Bit commitment from oblivious string transfer [CKS13])

1. *Commit phase: Alice and Bob perform the* OT_1^n *protocol such that Alice gets the output* $(z_0, z_1) \in \{0,1\}^n \times \{0,1\}^n$ *and Bob gets the output* $(b, w) \in \{0,1\} \times \{0,1\}^n$*. Here,* b *is the committed bit.*

2. *Reveal phase: If no one aborted, then Bob sends* (b, w) *to Alice.*

3. *If (b, w) from Bob is inconsistent with (z_0, z_1) then Alice aborts. Otherwise, she accepts b as the committed bit.*

We have $A_{\mathrm{OT}^n} = A_{\mathrm{BC}}$ since both are equal to the amount Alice can learn b from the OT_1^n protocol without Bob aborting. It is clear that Bob must send (c, z_c) if he wants to reveal c. Therefore, by letting q be the probability the OT_1^n is not aborted by Alice using Bob's optimal bit commitment strategy, we have $B_{\mathrm{BC}} = qc$, where

$$c = \frac{1}{2} \sum_{b \in \{0,1\}} \Pr[\text{Bob can learn } z_b | \text{Alice did not abort the } \mathrm{OT}_1^n \text{ protocol}].$$

From Theorem 1, we know that Bob has a strategy to learn (z_0, z_1) with probability

$$B_{\mathrm{OT}^n} \geq qc(2c-1)^2$$

noting that $B_{\mathrm{BC}} \geq 1/2 \implies c \geq 1/2$.

Fact 1 (Lower bound for bit commitment [CK11]) *For any bit commitment protocol, there is a parameter $t \in [0, 1]$ such that*

$$B_{\mathrm{BC}} \geq \left(1 - \left(1 - \frac{1}{\sqrt{2}}\right) t\right)^2 \quad \textit{and} \quad A_{\mathrm{BC}} \geq \frac{1}{2} + \frac{t}{2}.$$

Using Fact 1, this yields the lower bound $\max\{A_{\mathrm{OT}^n}, B_{\mathrm{OT}^n}\} \geq 0.5852$, which is independent of n. If $n = 1$, we can use the stronger bound in Theorem 1 to get

$$B_{\mathrm{OT}} \geq q(2c-1)^2$$

improving the lower bound to $\max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\} \geq 0.599$.

C Technical Claims

Claim 2 *Suppose $\theta, \tau \in [0, \pi/2]$ satisfy $\theta + \tau \leq \pi/2$. Then* $\cos(\theta + \tau) \geq \cos^2(\theta) + \cos^2(\tau) - 1$.

Proof Without loss of generality, suppose that $\theta \geq \tau$. Consider the function

$$f(\theta) = \cos(\theta + \tau) - \cos^2(\theta) - \cos^2(\tau) + 1$$

for fixed τ. Taking its derivative, we get $f'(\theta) = -\sin(\theta + \tau) + \sin(2\theta)$, which is nonnegative for $\theta \in [\tau, \pi/3 - \tau/3]$ and nonpositive for $\theta \in [\pi/3 - \tau/3, \pi/2 - \tau]$. Note that $\tau \leq \pi/3 - \tau/3 \leq \pi/2 - \tau$ since $\tau \leq \pi/4$. So we conclude that f is increasing on $[\tau, \pi/3 - \tau/3]$ and decreasing on $[\pi/3 - \tau/3, \pi/2 - \tau]$. Since $f(\tau) = 0$ and $f(\pi/2 - \tau) = 0$, we have that f is positive for $\theta \in [\tau, \pi/2 - \tau]$. If $\theta, \tau \in [0, \pi/2]$ with $\theta + \tau \leq \pi/2$ and $\theta \geq \tau$, we have exactly that $\theta \in [\tau, \pi/2 - \tau]$. We conclude from the positivity of f that $\cos(\theta + \tau) \geq \cos^2(\theta) + \cos^2(\tau) - 1$, as desired. □

Claim 3 *Let* $\theta, \tau \in [0, \frac{\pi}{2}]$ *satisfy* $\cos^2(\theta)+\cos^2(\tau) \geq 1$. *Then* $\cos(\theta+\tau) \geq \cos^2(\theta)+\cos^2(\tau)-1$.

Proof Since $\theta, \tau \in [0, \pi/2]$ satisfy $\cos^2(\theta) + \cos^2(\tau) \geq 1$, we have

$$\cos^2(\theta) + \sin^2(\theta) = 1 \leq \cos^2(\theta) + \cos^2(\tau) = \cos^2(\theta) + \sin^2(\pi/2 - \tau)$$

which gives directly $\theta \leq \pi/2 - \tau$, or equivalently, $\theta + \tau \leq \pi/2$. Claim 2 concludes the proof. □

D Bounding the value of CHSH_n using semidefinite programming

We discuss the tightness of our bound on CHSH_n, i.e., that

$$\omega^*(\mathrm{CHSH}_n) \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}.$$

This was proven using an equivalence to a Hidden XOR condition and subsequently by our Hidden XOR lemma. However, this is not the only way to bound the value of quantum games. For instance, one can upper bound the value of two-player, one-round games using semidefinite programming [KRT10]. We now compare our bound to the one given by semidefinite programs (SDPs).

We solved a relaxation[3] of this SDP to get numerical upper bounds on the value of CHSH_n for $n \in \{1, 2, 3, 4, 5\}$. These values can be found in Table 1 along with the values from our proven upper bound and the classical value lower bound.

Table 1: Bounds on the CHSH_n game for $n \in \{1, 2, 3, 4, 5\}$.

Value	$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$
Classical Value	0.7500	0.6250	0.5625	0.5312	0.5156
Conjectured Value	0.8535	0.7500	0.6767	0.6250	0.5883
SDP Relaxation	0.8535	0.7803	0.7437	0.7254	0.7163
Our Proven Bound	1	0.8535	0.7500	0.6767	0.6250

We can see that the SDP relaxation gives a tighter upper bound than ours for $n \leq 3$, but the numerical results suggest that our bound outperforms the SDP bound for larger values of n. This implies that neither our bound nor the SDP one can be optimal for all n. In fact, we have the following conjecture for the optimal value.

Conjecture 1 *For every* $n \in \mathbb{N}$, *the value of* CHSH_n *is* $\omega^*(\mathrm{CHSH}_n) = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2^n}}$.

This provides the correct value for $n = 1$ and is a stronger bound for all n. It remains open to show whether our conjectured value is a lower and/or an upper bound on the value of CHSH_n.

[3] This relaxation is faster to solve and gives the same numerical values as solving the semidefinite program for small values of n.